Configurazione del Laboratorio Virtuale

1. **Impostazione della Comunicazione tra le Macchine:**
   - Assicurarsi che le macchine Metasploitable e Kali Linux siano sulla stessa rete.
   - Eseguire il comando `ping` dalla macchina Kali Linux per verificare la comunicazione:

     ```
     bash
     ping [IP_di_Metasploitable]
     ```

2. **Accesso a DVWA:**
   - Aprire un browser su Kali Linux e navigare all'indirizzo della DVWA:

     ```
     arduino
     http://[IP_di_Metasploitable]/dvwa
     ```

   - Accedere con le credenziali predefinite (utente: `admin`, password: `password`).
   - Impostare il livello di sicurezza su "LOW" dalla scheda "DVWA Security".

Esecuzione di Attacchi XSS Reflected e SQL Injection

1. Attacco XSS Reflected

Obiettivo: Eseguire uno script JavaScript tramite una vulnerabilità XSS riflessa.

Passaggi:

1. **Navigare alla Pagina XSS Reflected:**
   - Andare alla scheda "XSS (Reflected)" su DVWA.
2. **Inserire il Payload XSS:**
   - Esempio di payload di base per XSS riflesso:

     ```
     html
     <script>alert('XSS');</script>
     ```

   - Inserire questo payload nel campo di input e inviare il modulo.
3. **Verifica dell'Attacco:**
   - Se l'attacco ha successo, si dovrebbe vedere un popup con il messaggio "XSS".

Payload Avanzati:

- Recupero del cookie:

  ```
  html
  <script>alert(document.cookie);</script>
  ```

- Iniettare contenuto HTML:

  ```
  html
  <i>Testo in corsivo</i>
  ```

Screenshot di Esempio:

- Screenshot che mostra il popup di JavaScript:
- Screenshot che mostra il recupero del cookie:

2. Attacco SQL Injection (Non Blind)

Obiettivo: Eseguire una query SQL malevola tramite una vulnerabilità SQL injection.

Passaggi:

1. **Navigare alla Pagina SQL Injection:**
   - Andare alla scheda "SQL Injection" su DVWA.
2. **Controllo di Vulnerabilità:**
   - Inserire un singolo apice `'` nel campo di input e inviare il modulo.
   - Se compare un errore SQL, significa che il campo è vulnerabile.
3. **Esempio di Attacco SQL Injection:**
   - Recuperare tutte le voci del database utilizzando l'operatore UNION:

     ```
     sql
     ' UNION SELECT null, database()--
     ```

   - Eseguire il payload inserendolo nel campo di input e inviare il modulo.

Union Attack Avanzato:

- Recuperare il nome dell'utente e la password:

  ```
  sql
  ' UNION SELECT user, password FROM users--
  ```

Screenshot di Esempio:

- Screenshot che mostra l'errore SQL:
- Screenshot che mostra i risultati dell'attacco UNION:

Creazione del Report PDF

XSS Reflected Report

1. **Introduzione all'Attacco XSS Reflected:**
   - Spiegazione di cosa è un attacco XSS riflesso e come funziona.
2. **Passaggi Eseguiti:**
   - Descrizione dei passaggi seguiti per eseguire l'attacco.
3. **Payload Utilizzati:**
   - Elenco dei payload XSS utilizzati con spiegazioni.
4. **Risultati dell'Attacco:**
   - Screenshot e descrizione dei risultati ottenuti con ogni payload.

SQL Injection Report

1. **Introduzione all'Attacco SQL Injection:**
   - Spiegazione di cosa è un attacco SQL injection e come funziona.
2. **Passaggi Eseguiti:**

    - Descrizione dei passaggi seguiti per eseguire l'attacco.
3. **Payload Utilizzati:**
    - Elenco dei payload SQL utilizzati con spiegazioni.
4. **Risultati dell'Attacco:**
    - Screenshot e descrizione dei risultati ottenuti con ogni payload.

Generazione dei Report PDF

Per generare i report PDF, si possono utilizzare strumenti come LibreOffice o altri editor di documenti che permettono di esportare i file in formato PDF. Assicurarsi di includere tutte le informazioni necessarie e gli screenshot per fornire un report completo e dettagliato.

Esempio di Codice per SQL Injection

```
sql
' UNION SELECT null, user()--
sql
Copia codice
' UNION SELECT null, database()--
sql
Copia codice
' UNION SELECT user, password FROM users--
```